RESPONSE UNDER 37 C.F.R. § 1.111
Application No. 09/716,273
Attorney Docket No.: Q61623

REMARKS

Claims 1-24 are all the claims pending in the application.

Summary of the Office Action

The Examiner withdrew the previous rejections. The Examiner, however, found new grounds for rejecting the claims. Claims 1-24 are rejected under 35 U.S.C. § 102(e).

Prior Art Rejections

Claims 1-24 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,571,221 to Stewart et al. (hereinafter "Stewart"). Applicant respectfully requests the Examiner to reconsider this rejection in view of the following comments.

To be an "anticipation" rejection under 35 U.S.C. § 102, the reference must teach every element and recitation of the Applicant's claims. Rejections under 35 U.S.C. § 102 are proper only when the claimed subject matter is identically disclosed or described in the prior art. Thus, the reference must clearly and unequivocally disclose every element and recitation of the claimed invention.

Claim 1, 8, 15, 22, and 23 are the only independent claims. This response focuses initially on these independent claims.

Independent claim 1, among a number of unique features not taught by the cited prior art reference, recites: "means for storing a current set of primary provisioning data; means for storing at least one set of protected primary provisioning data that cannot be updated without the intervention of the terminal user...wherein a connection to the data network is set up using the selected set of provisioning data." Applicant respectfully submits that Stewart fails to disclose

storing the current and protected set of certificates for data network access, and establishing a connection (setting up a connection) to the data network using the selected set of certificates.

An illustrative, non-limiting embodiment of the present invention, discloses a method and a telecommunications terminal operable to connect the device to a data network. The exemplary telecommunication terminal can change between access networks and/or users without loosing the provisioning data by storing a protected primary provisioning data or a number of sets of protected primary provisioning data that cannot be modified without intervention from the user. Thereby, in this exemplary telecommunication terminal, there is no need to update the provisioning data to access the services of a data network each time the user roams between access networks and/or users. It will be appreciated that the foregoing remarks relate to the invention in a general sense, the remarks are not necessarily limitative of any claims and are intended only to help the Examiner better understand the distinguishing aspects of the claims mentioned above.

Stewart is unrelated to providing a connection to the data network. Instead, Stewart relates to digital certificates *i.e.*, the use of digital certificates for the purposes of tracking sponsorship information or membership information of users of the network, as well as for computing billing services or network access services, and providing other services, based at least partly on the sponsorship information (col. 1, lines 10 to 14, *Field of the Invention*). Stewart's digital certificate is simply an attachment to an electronic message used for the security purposes such as to verify the user identity. That is, in Stewart, when a client or user accesses a

website, the client computer submits its digital certificate to the web server (col. 1, lines 15 to 58 and col. 11, lines 26 to 48).

However, prior to sending a certificate (*i.e.*, executing an online transaction), primary provisioning must be executed to allow the user to send the email. That is, prior to using Stewart's digital certificates, connection to an access point of the data network needs to be established. In other words, Stewart is unrelated to establishing a connection to the data network because it relates to digital certificates, which "are useful for performing secure electronic commerce (e-commerce) transactions, and may be used to uniquely identify users" (col. 1, lines 31 to 33).

With respect to connecting to an access network, Stewart only discloses that the user connects to the network *e.g.*, to an access point of the network. For example, the user may be walking in an airport with a portable computing device and may connect in a wireless fashion to an access point located at the airport. In another scenario, the user may enter a hotel room and connect to an Ethernet port in his/her room which is connected to the network. Thus, the user may connect to the network or an access point of the network in a wired or wireless fashion (col. 13, lines 22 to 63).

In short, if, as alleged by the Examiner, the digital certificates of Stewart disclose the primary provisioning data, then Stewart fails to disclose "wherein a connection to the data network is set up using the selected set of provisioning data." As the digital certificate of Stewart is not used to set up the connection.

Moreover, the Examiner alleges that Stewart discloses "means for storing a current set of primary provisioning data; means for storing at least one set of protected primary provisioning data that cannot be updated without the intervention of the terminal user (*see* page 2 of the Office Action). Applicant respectfully disagrees.

Stewart only discloses that a digital certificate may be stored on the mobile user's PCD in order to allow access to the network. When accessing the communication service network, the identity of the user may be established by the digital certificate stored on the user's computer. The digital certificate may also store sponsorship information, including information regarding programs or entities in which the mobile user is a member or is affiliated. The sponsorship information may also comprise references or cookies to more detailed sponsorship information, which may be kept on a separate server. The information may be stored in extensions within the digital certificate (col. 2, line 57 to col. 3, line 32).

Stewart, however, fails to disclose a current digital certificate and a protected digital certificate. Since Stewart only discloses the digital certificate being stored mobile user's PCD or some of it may be stored on a separate server, the rejection is improper as it lacks "sufficient specificity" required under 102. "[A]nticipation under § 102 can be found only when the reference discloses exactly what is claimed and that where there are differences between the reference disclosure and the claim, the rejection must be based on § 103 which takes differences into account." *Titanium Metals Corp. v. Banner*, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985); MPEP § 2131. Moreover, Stewart fails to disclose that the digital certificate "cannot be updated without the intervention of the terminal user."

For at least these exemplary reasons, claim 1 patentably distinguishes from Stewart. Claims 2-7 are patentable at least by virtue of their dependency on claim 1. Claims 8 and 15 recite features similar to, though not necessarily coextensive with, the features argued above with respect to claim 1. Therefore, arguments presented with respect to claim 1 are respectfully submitted to apply with equal force here. For at least substantially analogous exemplary reasons, independent claims 8 and 15 are patentably distinguishable from Stewart. Claims 9-14 and 16-21 are patentable at least by virtue of their dependency on claims 8 and 15, respectively.

Independent claim 22, among a number of unique features, recites: "backing up provisioning data for an access network, an access provider or a user." In Stewart, there is no disclosure of the backup. Indeed, Figs. 1-5 of Stewart do not disclose backing up data. For at least this exemplary reason, independent claim 22 patentably distinguishes from Stewart.

Independent claim 23, among a number of unique features, recites: "protecting the backed up provisioning data to prevent it being updated without the intervention of the user, an access network operator or the access provider." In Stewart, there is no disclosure of backed up digital certificate. In addition, there is no disclosure of protecting the backed up digital certificate. For at least these exemplary reasons, claim 23 patentably distinguishes from Stewart. Claim 24 is patentable at least by virtue of its dependency on claim 23.

In view thereof, Applicant respectfully requests the Examiner to withdraw this rejections of claims 1-24.

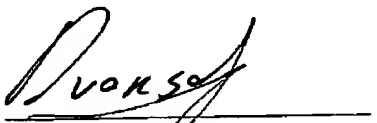
RESPONSE UNDER 37 C.F.R. § 1.111
Application No. 09/716,273
Attorney Docket No.: Q61623

Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly invited to contact the undersigned attorney at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,



Nataliya Dvorson
Registration No. 56,616

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: December 5, 2005